

REMARKS

In the Office Action, the Examiner rejected Claims 1-14, which were all of the then pending claims, over the prior art, including U.S. Patents 5,878,138 (Yacobi), 6,675,153 (Cook, et al.) and 5,627,893 (Demytko). More specifically, Claims 1 and 2 were rejected under 35 U.S.C. §102 as being fully anticipated by Yacobi; Claims 3-5, 7-9 and 11-13 were rejected under 35 U.S.C. §102 as being fully anticipated by Cook, et al; and Claims 6, 10 and 14 were rejected under 35 U.S.C. §103 as being unpatentable over Cook, et al. in view of Demytko.

Independent Claims 1, 3, 7 and 11 are being amended to better define the subject matters of these claims. Claims 6, 10 and 14 are being cancelled to reduce the number of issues. Also, new Claims 15 and 16, which are dependent from Claim 3, are being added to describe preferred feature of the invention.

For the reasons set forth below, Claims 1-5, 7-9, 11-13, 15 and 16 patentably distinguish over the prior art and are allowable. The Examiner is, accordingly, respectfully asked to reconsider and to withdraw the above-identified rejections of Claims 1-5, 7-9 and 11-13, and to allow these claims and new Claims 15 and 16.

The present invention, generally, relates to methods and systems to create and manage digital cash. In this system, a customer sends a request for digital cash to a bank along with a public key of an encryption scheme. The bank signs the cash using a secret key of a digital signature scheme, and then encrypts the signature by using the public key provided by the customer. The customer then decrypts the cash using the private key of the encryption scheme, and can then use the cash for payment to a third party. That third party is able to check the validity of the digital cash with the bank and can redeem the digital cash for payment.

An important feature of the invention is that the signature scheme used by the bank is non-homomorphic. This allows the customer to receive and use the cash, and allows the third party to redeem the cash, while keeping the identity of the customer secret from the bank. Moreover, all of this can be achieved without having to use a blind signature.

Yacobi and Cook, et al. disclose procedures for generating and using electronic cash or electronic assets.

In one procedure described in Yacobi, a temper resistant electronic wallet is used to store the asset. The wallet is designed to detect fraud and to eliminate further fraud before the criminal has had an opportunity to profit from the fraud.

Also, Yacobi discloses, from column 12, line 50 to column 15, line 10, a blind re-certification process; however, this process uses a blind signature, as specifically discussed in column 12, lines 50-64.

Cook, et al. discloses a procedure for authorizing electronic transactions between a consumer and a merchant. A goal of this procedure is to keep the consumer anonymous to the merchant, not to keep the consumer anonymous from the issuer or certifying authority.

Yacobi and Cook, et al. thus fail to disclose the above-discussed use of a non-homomorphic signature scheme by the entity issuing the digital cash.

Non-homomorphic signature schemes are, per se, known, and in the Office Action, the Examiner cited Demytko as disclosing such a scheme. Demytko does not relate to digital cash, and does not provide any suggestion or guidance as to how to use effectively the disclosed cryptographic method in a digital cash system

What the prior art fails to disclose or suggest, hence, is the use of a non-homomorphic signature scheme, in a digital cash system, to allow a customer to use the digital cash while keeping the identity of the customer secret from the bank or issuing authority.

Independent Claims 1, 3, 7 and 11 clearly describe this feature of the invention. In particular, Claim 1 describes the feature that the coin – that is, the digital cash – is signed with a non-homomorphic signature to enable the user to use the coin while keeping the user unknown to the coprocessor that signs the coin. Similarly, Claims 2, 7 and 11 describe the feature that the unit, which represents the electronic cash, is signed with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the co-processor that signs the unit.

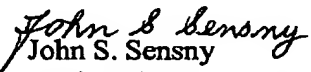
This feature of the invention is of utility because, as mentioned above, it enables the customer to remain anonymous to the issuing entity and without requiring a blind signature scheme.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not suggest or disclose the use of a non-homomorphic signature in the above-described manner.

Because of the differences between Claims 1, 3, 7 and 11, and because of the advantages associated with those differences, Claims 1, 3, 7 and 11 patentably distinguish over the prior art and are allowable. Claim 2 is dependent from, and is allowable with, Claim 1; and Claims 4, 5, 15 and 16 are dependent from Claim 3 and are allowable therewith. Likewise, Claims 8 and 9 are dependent from Claim 7 and are allowable therewith; and Claims 12 and 13 are dependent from, and are allowable with, Claim 11. The Examiner is, accordingly, respectfully requested to reconsider and to withdraw the rejections of Claims 1-5, 7-9 and 11-13 under 35 U.S.C. §102, and to allow these claims and new Claims 15 and 16.

Every effort has been made to place this application in condition for allowance, a notice of which is requested. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,


John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser
400 Garden City Plaza
Garden City, New York 11530

JSS:jy